EXPRESS MAIL NO. EV447226056US

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 7/16, H04L 9/08 — A1

(11) International Publication Number: **WO 00/59222**

(43) International Publication Date: 5 October 2000 (05.10.00)

(21) International Application Number: PCT/US00/05111

(22) International Filing Date: 29 February 2000 (29.02.00)

(30) Priority Data:

60/126,805	30 March 1999 (30.03.99)	US
09/497,393	3 February 2000 (03.02.00)	US

(71) Applicant: SONY ELECTRONICS, INC. [US/US]; 1 Sony Drive, Park Ridge, NJ 07656 (US).

(72) Inventor: CANDELORE, Brant, L.; 10124 Quail Glen Way, Escondido, CA 92029 (US).

(74) Agents: SOBRINO, Maria, E. et al.; Blakely, Sokoloff, Taylor & Zafman, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025-1026 (US).

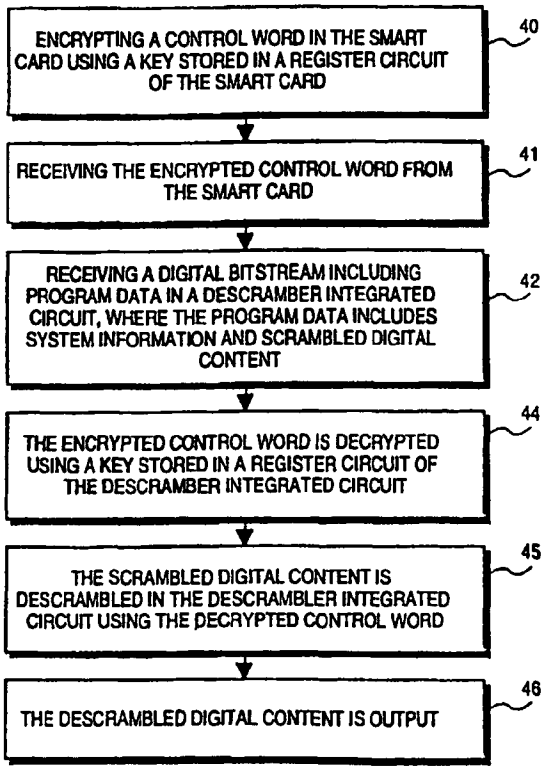
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD AND APPARATUS FOR SECURING CONTROL WORDS

(57) Abstract

In accordance with one embodiment, a method for securing control words is provided. The method includes (42) receiving scrambled digital content in a descrambler integrated circuit. The method further includes (41) receiving an encrypted control word in the descrambler integrated circuit, (44) decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and (45) descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD AND APPARATUS FOR SECURING CONTROL WORDS

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit of U.S. provisional application U.S. Serial No. 60/126,805, filed on March 30, 1999, entitled "Method For Securing Control Words and Cost Reducing a Set Top Box."

BACKGROUND OF THE INVENTION

1. *Field of the Invention*

The present invention relates to digital devices. More specifically, the present invention relates to an apparatus and method for descrambling digital content in digital devices.

2. *General Background*

Analog communication systems are rapidly giving way to their digital counterparts. Digital television is currently scheduled to be available nationally to all consumers by the year 2002 and completely in place by the year 2006. High-definition television (HDTV) broadcasts have already begun in most major cities on a limited basis. Similarly, the explosive growth of the Internet and the World Wide Web have resulted in a correlative growth in the increase of downloadable audio-visual files, such as MP3-formatted audio files, as well as other content.

Simultaneously with, and in part due to, this rapid move to digital communications system, there have been significant advances in digital recording devices. Digital versatile disk (DVD) recorders, digital VHS video cassette recorders (D-VHS VCR), CD-ROM recorders (e.g., CD-R and CD-RW), MP3 recording devices, and hard disk-based recording units are but merely representative of the digital recording devices that are capable of producing high quality recordings and copies thereof, without the generational degradation (i.e., increased degradation between successive copies) known in the analog counterparts. The combination of movement towards digital communication systems and digital recording devices poses a concern to content providers such as the motion picture and music industries, who desire to prevent the unauthorized and uncontrolled copying of copyrighted, or otherwise protected, material.

In response, there is a movement to require service providers, such as terrestrial broadcast, cable and direct broadcast satellite (DBS) companies, and companies having Internet sites which provide downloadable content, to introduce protection schemes. Two such copy protection systems have been proposed by the 5C group of the Data Hiding Sub Group (DHSG) (5C comprising representatives of Sony, Hitachi, Toshiba, Matsushita, and Intel) and the Data Transmission Discussion Group (DTDG), which are industry committee sub-groups of the Copy Protection Technical Working Group (CPTWG). The CPTWG represents the content providers, computer and consumer electronic product manufacturers.

The DTDG Digital Transmission Copy Protection (DTCP) proposal is targeted for protecting copy-protected digital content, which is transferred between digital devices connected via a digital transmission medium such as an IEEE 1394 serial bus. Device-based, the proposal uses symmetric key cryptographic techniques to encode components of a compliant device. This allows for the authentication of any digital device prior to the transmission of the digital content in order to determine whether the device is compliant. The digital content is itself encoded prior to transmission so that unauthorized copying of the content will result in copy having an unintelligible format.

One method of encoding the content has been proposed by the DHSG, and is based on watermarking techniques. Although the main focus of the DHSG proposal has been for copy protection of digital movie and video content, particularly as applied to DVD systems, it is expected to be applicable to the copy protection of any digital content distributed electronically via digital broadcasts and networks. The watermarking techniques, which are invisible to the user, allow the incoming content to be marked in a manner that makes it extremely difficult to discern precisely how the content was encoded, and thus extremely difficult to remove or alter the watermark without damaging the content. The DHSG has determined three primary cases of detection and control that such a technology should accomplish: playback, record and generational copy control. It is anticipated that the watermarking technology will allow the content provider to specify at least whether the content is "copy never," "copy once," and "copy free" content. "Copy never" is used to mark digital content to

indicate that the content is not allowed to be copied, while "copy free" indicates that the content may be copied freely and which can be marked with additional information. This is different than material that is never marked. Finally, "copy once" is used to indicate that the digital content is allowed to be copied only once. As a copy is being made, the original "copy once" content and the newly copied content are re-marked with "no more copy." Of course, other types of copy management commands may limit the playing or reproduction of such digital content; for example, to a specific period of time, duration, or number of plays or viewings.

Thus, even today, the functionality of digital devices such as set-top boxes, digital televisions, digital audio players, and similar such digital devices extends beyond their historical role of conditional access (CA), i.e., merely descrambling content to a CA-clear format for real-time viewing and/or listening, and now include constraints and conditions on the recording and playback of such digital content. For example, currently, copying of scrambled content for subsequent descrambling and viewing or listening may be permitted with the appropriate service/content provider authorization or key provided to the digital device

Traditional conditional access systems for Pay-TV originated from one-way broadcast systems where a back channel was not available. A cryptographic processor, such as a smart card, in a conditional access unit, such as a set top box, for example, is generally infused with information and functionality in order to automatically grant access to programs.

For example, a smart card with a Pay-TV access control application typically receives EMMs which grant certain service entitlements. Typically, services or group keys are delivered at the same time, and if the set top box is allowed to view IPPV programs, then credit and cost limit information may be transmitted as well.

When tuning to a program, the smart card receives ECMs which describe which entitlements the smart card needs in order to grant access to the show. Hackers may attempt to manipulate both EMMs and ECMs to view programs without paying the requisite subscription fees. Not only are the EMMs and ECMs manipulated, but the hardware is attacked as well. This combination of

software and hardware attacks are used to cause the smart card to decrypt scrambled programs without authorization from the provider of the programs.

Once fielded, it is hard to change the functionality of the smart cards. Mechanisms for downloading new code to smart cards are prone to attack by hackers who may try to use the same mechanisms to load pirate code into the smart card in order to steal programs. One "safe" way to upgrade the access control system is to remove existing smart cards from the field and provide new ones. However, this can be costly and logistically difficult.

SUMMARY

In accordance with one embodiment, a method for securing control words is provided. The method includes receiving scrambled digital content in a descrambler integrated circuit. The method further includes receiving an encrypted control word in the descrambler integrated circuit, decrypting the encrypted control word using a key stored in a register circuit of the descrambler integrated circuit, and descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not by way of limitation in the figures of the accompanying drawings, in which like references indicate similar elements and in which:

Figure 1 is a block diagram of an exemplary entertainment system including one embodiment of a digital device;

Figure 2 is an embodiment of a conditional access unit with a smart card;

Figure 3 is an embodiment of a method for securely transferring control words from a smart card to a conditional access unit;

Figures 4 and **5** are embodiments of a method for encrypting and decrypting data;

Figure 6 is a block diagram of an embodiment of the descrambler integrated circuit;

Figure 7 is an embodiment of a headend server, network connection, and decoder;

Figure 8 is another embodiment of a decoder;

Figure 9 show embodiments of services that may be delivered to a decoder or a conditional access unit; and

Figure 10 shows an embodiment of a method for requesting and receiving control words or service keys.

DETAILED DESCRIPTION

Figure 1 is a block diagram of an entertainment system 100 including one embodiment of the copy management system of the present invention. The entertainment system 100 includes a digital device 110 for receiving a digital bitstream including program data from one or more service providers. Such service or content providers can include terrestrial broadcasters, cable operators, direct broadcast satellite (DBS) companies, companies providing content for download via the Internet, or any similar such content and/or service provider. The program data may include system information, entitlement control messages, entitlement management messages, content, and other data, each of which will be described briefly. System information may include information on program names, time of broadcast, source, and a method of retrieval and decoding, and well as copy management commands that provide digital receivers and other devices with information that will control how and when program data may be replayed, retransmitted and/or recorded. These copy management commands may also be transmitted along with entitlement control messages (ECM), which are generally used by the conditional access unit to regulate access to a particular channel or service. Entitlement management messages (EMM) may be used to deliver privileges to the digital receiver 111 such as rights, access parameters, and descrambling keys. As known, a decryption key is generally a code that is required to restore scrambled data, and may be a function of the rights granted. Finally, content in the program data stream may include audio and video data, which may be in a scrambled or clear format.

The digital device 110 includes a digital receiver 111, which processes the incoming bitstream, extracts the program data therefrom, and provides the program data in a viewable format. Digital device 110 may be coupled to other components in the entertainment system 100 via a transmission medium 120. The transmission medium 120 operates to transmit control information and data including program data between the digital device 110 and other components in the entertainment system 100.

The entertainment system 100 may include an audio system 130 coupled to the transmission medium 120. A digital VCR 140, such as a D-VHS VCR, may also be coupled to the digital device 110 and other components of the entertainment system 100 through the transmission medium 120.

A hard disk recording unit 150 may also be coupled to digital device 110 and other components via transmission medium 120. Display 160 may include a high definition television display, a monitor or other device capable of processing digital video signals. Finally, a control unit 170 may be coupled to the transmission medium 120. The control unit 170 may be used to coordinate and control the operation of some or each of the components on the entertainment system 100.

The content of a digital program may be transmitted in scrambled form. In order for a conditional access unit to recover the scrambled content and permit a person to view the content in clear form, the unit must have the necessary access requirements associated with the scrambled content. An access requirement includes a message that describes the features that the conditional access unit must have in order to decode the scrambled content. For example, a certain key may be needed to view the content. Alternatively, a service tag associated with a given content provider may be required. Technical requirements such as a particular descrambling method may also be required and included as a part of the access requirements. The access requirements associated with a particular program may be transmitted to a conditional access unit along with the program.

When a scrambled program is received by a conditional access unit, the access requirements for the program are compared to the entitlements that the conditional access unit actually has. In order for the conditional access unit to

display the scrambled content in clear form, the access requirements for the program must match the entitlements of the conditional access unit. The entitlements may state that the conditional access unit is entitled to view content from a given service provider such as HBO, for example. The entitlements may also include one or more keys needed to descramble the content. The entitlements also may define the time periods for which the conditional access unit may descramble programs. The access requirements and entitlements thus form a part of the access control system to determine whether a decoder is authorized to view a particular program.

The access requirements and entitlements can provide consumers with a variety of choices for paying for the content and gaining access to the scrambled content. These choices may include pay per play (PPP), pay per view (PPV), impulse pay per view (IPPV), time based historical, pay per time (PPT), repurchase of copy never movies, personal scrambling, and regional pay per view. Impulse pay per view is a feature which allows purchase of pay per view movies through credit that has been previously downloaded into the set top box. Purchase records may be stored and forwarded by phone to a billing center. Time based historical allows access to content that was delivered during a past time period, such as March through December, 1997, for example. The access requirements and entitlements can also provide consumers with different options for storing the scrambled content.

The access requirements may be delivered to the conditional access unit using packet identifiers (PIDs). Each PID may contain the access requirements associated with a given service or feature. The content that is delivered to a conditional access unit may also include a large number of PIDs, thus enabling special revenue features, technical features, or other special features to be performed locally.

Before receiving the content, the customer may be given a number of choices for gaining access to the content that is going to be stored to media. The customer may be required to purchase the right to access and view the content. Therefore, if the customer wants to record the content for later retrieval and viewing, the access requirements that the customer bought also need to be stored with the content.

There are different types of security architectures for conditional access units: 1) embedded; 2) split security; and 3) external security. With embedded security, the content descrambling and the key management is done all within the conditional access unit, such as a set top box for example. With split security, the descrambling is done within the set top box, but the key management is performed external to the set top box, by using a cryptographic processor such as a smart card. With external security, both the content descrambling and the key management are performed externally, such as with the NRSS-A and NRSS-B conditional access specifications. The cable industry through the Open Cable process has a modified version of NRSS-B called "Point-of-Deployment" (POD) module. The POD module has the same form factor as NRSS-B. It includes functionality for sending and receiving messages on the Out-of-Band channel. The external security type may also be split, for example, by using a PCMCIA form factor card that descrambles content, and a smart card that performs the key management.

In addition, there may be copy-protection applied to the CA descrambled transport stream. Copy-protected content will be re-scrambled across the CA module (NRSS-A, NRSS-B or POD) interface and the host. The CA element and the Host need to agree on the key used to re-encrypt this content. In one embodiment, various parameters are securely shared on each side of the interface, with the result that the same copy-protection key is derived by each party. The CA module can alternatively derive its own key and encrypt the copy protection key with the unique key of the descrambler integrated circuit in the host. The CA module can receive this unique key of the descrambler integrated circuit through an EMM or other method, e.g. factory load procedure.

As seen in **Figure 2**, an embodiment of the digital receiver 111 having the copy management system of the present invention includes a smart card interface 420. Although the smart card interface 420 may be built into the digital receiver 111, it is expected that digital receiver will have an expansion slot, such as a PCMCIA slot or Universal Services Bus (USB) slot to receive a card or device which includes the interface 420. The digital receiver 111 of this embodiment includes a CPU 430 and a descrambler integrated circuit 440.

Smart card interface 420 receives a smart card including encrypted control words for descrambling scrambled program content. Smart card 410 may transmit the control words in encrypted form to the smart card interface 420. If the content was originally scrambled using control words in addition to keys, the smart card 410 may use an encryption control key unique to unit 401 to encrypt the control words. The conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content.

Thus, **Figure 2** shows an embodiment of the split security architecture and the external architecture. In the split security architecture, conditional access unit 401 is a set top box or other type of digital device, such as device 110 shown in **Figure 1**. In the external architecture, conditional access unit 401 is a NRSS-B conditional access unit. An external cryptographic processor 410, such as an ISO 7816 smart card for example, receives control words (CWs) needed to descramble a program. The smart card 410 encrypts the CWs in encryption block 414 with keys that are unique to transport descrambler integrated circuit (IC) 440.

Smart card 410 delivers the encrypted CWs to the set top CPU 430 through interface 420. The transport descrambler IC 440 in the set top box 401 will decrypt the CWs using the unique descrambler IC keys stored in register 450. The decryption block 460 then writes the decrypted CWs alternately into ODD and EVEN key registers of descrambler 470 located in the transport descrambler chip 440. The descrambler 470 then applies the ODD/EVEN CWs to the scrambled content 480 at the right time and outputs descrambled program content 490.

Thus, the transfer of the control word from the smart card to the set top box is secure, because the control word is transferred in encrypted form. The control word remains secure in the set top box because the control word is not decrypted by the non secure processor 430. The control word is only decrypted in the descrambler IC 440 that actually uses the control word, therefore, the control word is never exposed, and cannot be obtained by hackers.

Furthermore, the key used to decrypt the control word is stored in hardware in register 450 in IC 440. The register 450 cannot be hacked unless

the silicon is probed and the register is destroyed. An attempt may be made to exhaustively trial the key stored in register 450 in IC 440. However, if the key is sufficiently large, the means of attack will be deemed hopeless. Furthermore, the key may only be valid for one particular unit 401, and may not be used by other units to decrypt control words, because the control words are encrypted by the smart card using a key that is unique to an associated conditional access unit 401. Therefore, the transmission of the encrypted control words from smart card 410 to conditional access unit 401 is secure and the control words are not vulnerable to theft by hackers.

The secure chip 440 does all of the secure processing of the control words. This secure chip has no CPU, no firmware, and no software. There is no complicated key hierarchy. A non CPU based descrambler chip receives the encrypted control words, applies a unique key to them, and decrypts them. No instructions, no code, no hashing, and no software is loaded into the decryption block. The decryption is performed entirely by a hardware circuit using only a single key function.

The Unique Keys may be programmed into register 450 during manufacture. For example, in one embodiment, the descrambler IC has a non-volatile Unique Key register 450 that can be written only once. When the set top, TV, or NRSS-B module 401 is manufactured, the Unique Key register 450 is programmed. In this embodiment, there is no way to either read or overwrite the original keys that were loaded into register 450. An association between the host's (401) serial number and the Unique Key that was loaded the Descrambler IC of that host may be recorded.

When the set top 401 is manufactured and a smart card 410 is installed, the smart card 410 can receive the Unique Key associated with unit 401 at the time of pairing. From then on, the smart card is "paired" to that particular host 401. Later, if the smart card 410 is ever replaced or moved to a new host, the smart card may receive the Descrambler IC Unique Keys in an Entitlement Management Message (EMM). New smart cards with the Unique Keys already programmed into the card may also be delivered to users.

A method for transferring the CWs from the smart card to the conditional access unit is shown in **Figure 3**. A control word is encrypted in the smart card

using a key stored in a register circuit of the smart card, step 40. The key stored in the register circuit of the smart card is associated with the key stored in the register circuit of the descrambler integrated circuit. The encrypted control word is received from the smart card, step 41. This method includes receiving a digital bitstream including program data in a descrambler integrated circuit, where the program data includes system information and scrambled digital content, step 42. The encrypted control word is decrypted using a key stored in a register circuit of the descrambler integrated circuit, step 44. The scrambled digital content is descrambled in the descrambler integrated circuit using the decrypted control word, step 45, and the descrambled digital content is output, step 46.

Embodiments of the encryption and decryption functions performed by encryption block 414 and decryption block 460 are shown in **Figures 4, 5** and **6**. These operations transform the CWs based on the Unique Keys stored in registers 412 and 450. An encryption algorithm such as DES, M6, or DVB Common Scrambling Algorithm may be used. In the embodiments shown in **Figures 4, 5** and **6**, Triple DES is used. As shown in **Figure 6**, the descrambler IC 440 uses Triple DES to decrypt the control words in decryption block 460. The decrypted control words are then used by descrambler 470 to descramble the program content 480 and output clear program content 490.

However, because the encryption and decryption of the CWs is local to the set top box, it is possible to phase in the deployment of increasingly more robust encryption. For example, single DES may be initially deployed, and later double or triple DES can be phased in with no consequence to already fielded paired units of set tops and smart cards. The key length of the Unique Keys may be at least as large as the descrambling Control Words, to help reduce attacks on the Unique Keys by hackers.

In an alternative embodiment as shown in **Figure 7**, the smart card may be replaced by the headend 710 of a one- or two-way network 720. The headend maintains the access rights for the decoder 701 instead of a local crypto microcontroller. The headend 710 can deliver Service Keys based on the Unique Keys stored in the Descrambler IC 740. The encrypted Service Keys

may be stored locally in the host 701 to facilitate transitions from one channel to another. The keys are stored in encrypted form, and are loaded as needed into the Descrambler IC 740. The Keys are decrypted only in the Descrambler IC 740, by using the Descrambler IC Unique Keys stored in register 750. In one embodiment, the service keys are used as Control Words to decrypt the content directly. In another embodiment, the Service Keys are used to decrypt control words, which are received in-band with the content.

The Service Keys may be encrypted and decrypted using one of the algorithms used for the control words in the embodiments of **Figures 2, 4, 5** and **6** described above. The algorithm used to encrypt and decrypt the Service Keys may be different than the algorithm used to scramble and descramble the program content. For example, M6 may be easier to do in software in either the smart card or the headend key server. Also, each Service Key may be encrypted using different public and proprietary encryption algorithm. These different proprietary algorithms may be considered as any-piracy measures to invalidate clone hardware.

The headend 710 can deliver Services Keys on a channel or tier of service basis in EMMs. The Services Keys are encrypted, stored locally in decoder 401 and used by the insecure processor 730 as needed when tuning to different channels. Because the set tops are fielded in high volume as compared to the headend, eliminating the cryptographic processors, such as smart cards, from the set tops can greatly reduce the cost of implementing a pay-TV system in a network.

While this embodiment works in one-way (non-IPPV) broadcast networks, it also performs in two-way, interactive networks, where the keys for a particular service are requested, such as IPPV or VOD purchases or any other non-subscription service. The return channel 721 requests the keys because the ability to grant access to a new service is performed by the headend 710 instead of a local controlling crypto-processor.

In order to avoid overload problems at the headend caused by a large number of simultaneous impulse buys of IPPV programs, a Free Preview period can be determined and IPPV programs can be marketed in advance of the actual viewing. In this embodiment, Service Keys for individual shows or movies

may be requested by unit 701 and delivered ahead of time. For example, interactive networks, such as a cable system having a back channel 721 such as a DOCSIS modem or Out-of-Band transmitter/receiver can deliver the request from the unit 701 to the headend 710. Alternatively, the set top unit 701 may request the current decryption service key for each program accessed.

A controller on the network headend server 710 processes this Request for Program Key (RPK). The request may contain the decoder's Unit Address, and information needed to identify the channel to be viewed (all of which may be obtained from MPEG system and program information already processed by the insecure processor). The request may be encrypted, if need be, for non-repudiation and prevention of denial of service attacks, such as IPPV or VOD requests for example.

Upon receipt of the message, the key server 710 looks up the decoder 701 in the access control list (listing each unit's entitlements) and verifies the decoder's authorization. If authorized, the controller send the Service Key (encrypted under the decoder's Unique Key located in the Descrambler IC) to the unit. **Figure 8** shows an alternative embodiment of decoder 701 that can request and receive service keys.

In this embodiment, the Service Key may be valid for a certain period of time. The decoder 701 may store the key as it surfs to other services, allowing the decoder to re-access the service with a still valid key without having to request the key again. In this embodiment, the key is stored in its unit specific encrypted form (as it comes over the network from the Key Server) in the memory 735 of the insecure processor 730 (which runs the decoder).

By using the memory and the processing power of the insecure, general purpose, host processor and not a separate cryptographic processor, a great cost reduction can be achieved. Not only can the cryptographic processor be eliminated, but there is also less overhead on the part of the host processor in dealing with communication to that cryptographic processor.

The Service Key may be valid for the duration of a program or it may be valid for a period of time, e.g. 6 hours. Using a key for a longer period of time will reduce the overall number of transactions between the decoder 701 and the headend 710 because once the key is stored in decoder 701, it is available to

the decoder from the decoder's memory. Depending on the duration of the current Service Key, the next key may be delivered along with the current key. Alternatively, the decoder may request the next Service Key after detecting the end of the current Service Key's valid Epoch. In one embodiment, the Service Key is valid for the duration of a user's subscription period.

The Service Key must be identified properly so that it may be applied to a channel being tuned to. When the set top box 701 tunes to a channel, it looks up the appropriate encrypted Service Key from memory 735 and writes that into the Odd/Even MPEG key register of the descrambler IC 740. As in the embodiment of **Figure 2**, the secret Unique Key information may be programmed into IC 740 when decoder 701 is manufactured.

In one embodiment, the Service Keys may comprise 56-bit, 112-bit, or 168-bit keys. Table 1 shows the storage requirements for different sizes of keys.

Table 1: Number of Bytes to Store Independent Service Keys

of Channels with Independent Keys	Channel ID (3 Bytes)	16 Byte Triple DES Encrypted Service Key	16 Byte Triple DES Encrypted Service Key	Total Bytes
		CURRENT	NEXT	
20	60	320	320	700
50	150	800	800	1,750
100	300	1600	1600	3,500
200	600	3200	3200	7,000
400	1200	6400	6400	14,000

Services can be sold a-la-carte or sold as a bouquet or package. There may be several tiers of services. For example, there may be a basic tier of services, a medium tier offering more services, and advanced tiers offering different premium services, as shown in **Figure 9**. In this embodiment, each incremental tier of services may be given a separate key.

From Table 1 above, if a customer where to subscribe to 20 different types of Service tiers, that would require 60 bytes of ID storage, 320 bytes of storage of the currently valid Service Keys, 320 bytes of storage for the Service Keys valid for the next epoch (or billing period) for a total of 700 bytes.

Typically, ECMs need to convey the Access Conditions needed to access a channel along with the Channel or Service ID information and Control Word (key) information. In this embodiment, the ECMs can be simplified. Only the Channel or Service ID information, and possibly Program ID if it is a IPPV or VOD program, need to be included in the ECM. This is because no ECM processing other than identifying the appropriate encrypted key from memory, and using it to write it into the appropriate register of the Descrambler IC needs to be performed.

Figure 10 shows one embodiment of a method for requesting and receiving service keys. Program information is continuously sent from the headend to the decoder, steps 1010 and 1015. A viewer then selects a channel to watch, step 1020. the decoder requests a Service Key from the headend, step 1025. The headend checks the subscription status of the decoder, step 1030. If the decoder is subscribed, the headend provides the Service Key to the decoder, step 1055. If the decoder is not subscribed, the viewer is asked by the decoder to subscribe, 1035. The viewer decides to subscribe, 1040. The decoder sends a request for purchase to the headend, 1045. The headend sends an encrypted Service Key to the decoder, 1050.

Thus, in this embodiment, the decoder includes a Descrambler IC with a Unique Key. Service Keys are delivered to decoder 701 encrypted by the descrambler IC Unique Key and stored in encrypted form in the decoder. Alternatively, the decoder could request a service key each time that the decoder tunes to a channel without storing service keys locally. The Entitlements normally held by the secure cryptographic processor are held by the controlling authority, e.g. a key server in the headend. The insecure processor 730 in decoder 701 may receive a message (e.g., an ECM or an EMM) which tells it what it is authorized to descramble so that it may properly display viewing options to a viewer. The processor 730 can then request service keys for selected channels. In this embodiment, there is no embedded "secure"

Firmware or software. Using the hardware decryption circuit mentioned above, an embedded CPU core or firmware that performs a cryptographic function is not needed. This enables a number of conditional access applications which may be downloaded to the insecure processor. The Service Key is unit key encrypted. It may be a public asymmetric key or secret symmetric key.

Additional advantages include Pay-TV applications without using a Cryptographic Processor by providing a decoder having a Descrambler IC with Unique Keys hardwired into the IC. The decoder can request a service key or control word from a network provider. Local Access control can be performed by the Insecure Processor because the critical "secure" function is isolated in the Descrambler IC.

In the foregoing description, the invention is described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the present invention as set forth in the appended claims. The specification and drawings are accordingly to be regarded in an illustrative rather than in a restrictive sense.

IN THE CLAIMS

What is claimed is:

1. A method of descrambling digital content comprising:

receiving scrambled digital content in a descrambler integrated circuit

receiving an encrypted control word in the descrambler integrated circuit;

decrypting the encrypted control word using a key stored in the descrambler integrated circuit; and

descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word.

2. The method of claim 1, wherein the digital content is content contained in a television transmission.

3. The method of claim 1, wherein the digital content is content downloaded from the Internet.

4. The method of claim 1, wherein the control word is decrypted using Triple DES.

5. The method of claim 1, wherein the encrypted control word is received from a smart card.

6. The method of claim 5 further comprising encrypting the control word in the smart card using a key stored in a register circuit of the smart card, wherein the key stored in the register circuit of the smart card is associated with the key stored in the register circuit of the descrambler integrated circuit.

7. The method of claim 1, wherein the encrypted control word is received from a controlling entity connected to the descrambler integrated circuit by a network.

8. The method of claim 7, wherein the controlling entity is selected from the group comprising a headend server, an uplink, or a broadcast station.

9. The method of claim 7 wherein the control word is encrypted by the controlling entity using a key associated with the key stored in the register circuit of the descrambler integrated circuit.

10. The method of claim 1, wherein the encrypted control word is received from a module.

11. The method of claim 10, wherein the module is selected from the group comprising an NRSS-A module, an NRSS-B module, a POD module, and other CA element.

12. An apparatus of descrambling digital content comprising:

means for receiving scrambled digital content in a descrambler integrated circuit;

means for receiving an encrypted control word in the descrambler integrated circuit;

means for decrypting the encrypted control word using a key stored in the descrambler integrated circuit; and

means for descrambling the scrambled digital content in the descrambler integrated circuit using the decrypted control word.

13. The apparatus of claim 12, wherein the digital content is content contained in a television transmission.

14. The apparatus of claim 12, wherein the digital content is content downloaded from the Internet.

15. The apparatus of claim 12, wherein the control word is decrypted using Triple DES.

16. The apparatus of claim 12, wherein the encrypted control word is received from a smart card.

17. The apparatus of claim 16 further comprising encrypting the control word in the smart card using a key stored in a register circuit of the smart card, wherein the key stored in the register circuit of the smart card is associated with the key stored in the register circuit of the descrambler integrated circuit.

18. The apparatus of claim 12, wherein the encrypted control word is received from a controlling entity connected to the descrambler integrated circuit by a network.

19. The apparatus of claim 18, wherein the controlling entity is selected from the group comprising a headend server, an uplink, or a broadcast station.

20. The apparatus of claim 12 wherein the control word is encrypted by the controlling entity using a key associated with the key stored in the register circuit of the descrambler integrated circuit.

21. The apparatus of claim 20, wherein the encrypted control word is received from a module.

22. The apparatus of claim 18, wherein the module is selected from the group comprising an NRSS-A module, an NRSS-B module, a POD module, and other CA element.

23. An apparatus of descrambling digital content comprising:

a descrambler integrated circuit;

a receiver scrambled digital content in a descrambler integrated circuit, and to receive an encrypted control word in the descrambler integrated circuit;

a decrypter the encrypted control word using a key stored in the descrambler integrated circuit; and

a descrambler the scrambled digital content in the descrambler integrated circuit using the decrypted control word.

24. The apparatus of claim 23, wherein the digital content is content contained in a television transmission.

25. The apparatus of claim 23, wherein the digital content is content downloaded from the Internet.

26. The apparatus of claim 23, wherein the control word is decrypted using Triple DES.

27. The apparatus of claim 23, wherein the encrypted control word is received from a smart card.

28. The apparatus of claim 27 further comprising encrypting the control word in the smart card using a key stored in a register circuit of the smart card, wherein the key stored in the register circuit of the smart card is associated with the key stored in the register circuit of the descrambler integrated circuit.

29. The apparatus of claim 23, wherein the encrypted control word is received from a controlling entity connected to the descrambler integrated circuit by a network.

30. The apparatus of claim 29 wherein the control word is encrypted by the controlling entity using a key associated with the key stored in the register circuit of the descrambler integrated circuit.

31. The apparatus of claim 23, wherein the encrypted control word is received from a module.

32. The apparatus of claim 31, wherein the module is selected from the group comprising an NRSS-A module, an NRSS-B module, a POD module, and other CA element.

33. The apparatus of claim 29, wherein the controlling entity is selected from the group comprising a headend sever, an uplink, or a broadcast station.

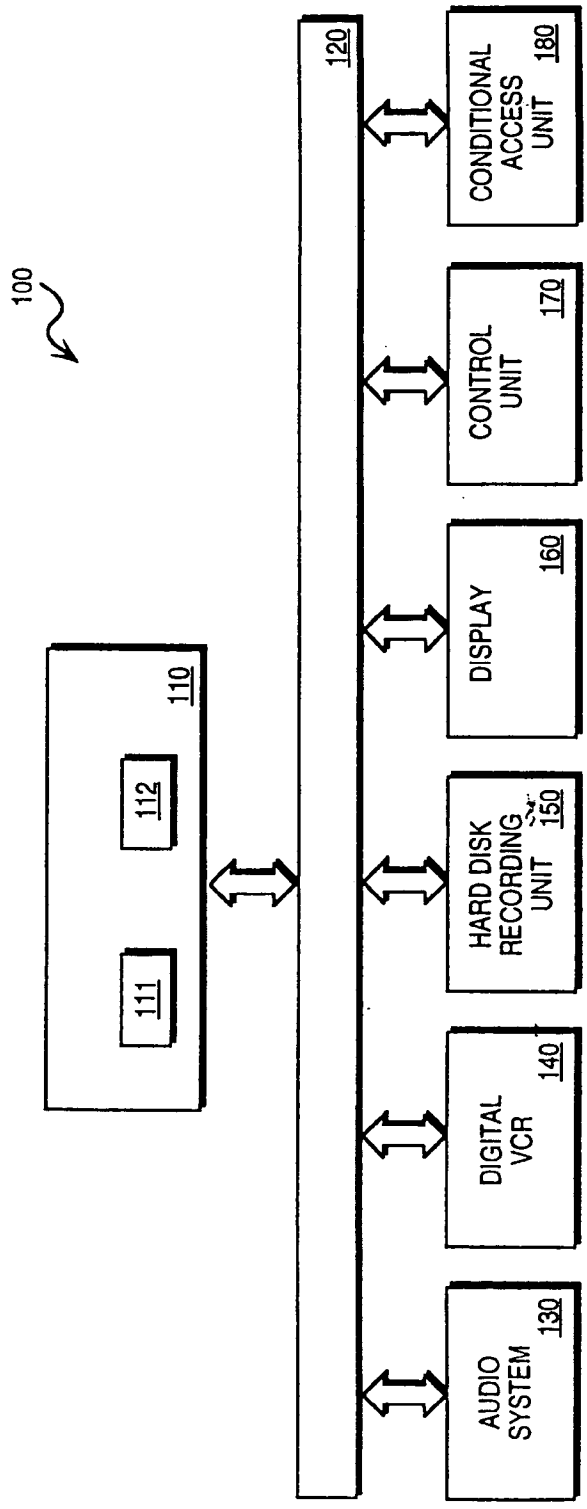

100
110
111
112
120
AUDIO SYSTEM 130
DIGITAL VCR 140
HARD DISK RECORDING UNIT 150
DISPLAY 160
CONTROL UNIT 170
CONDITIONAL ACCESS UNIT 180

FIG. 1

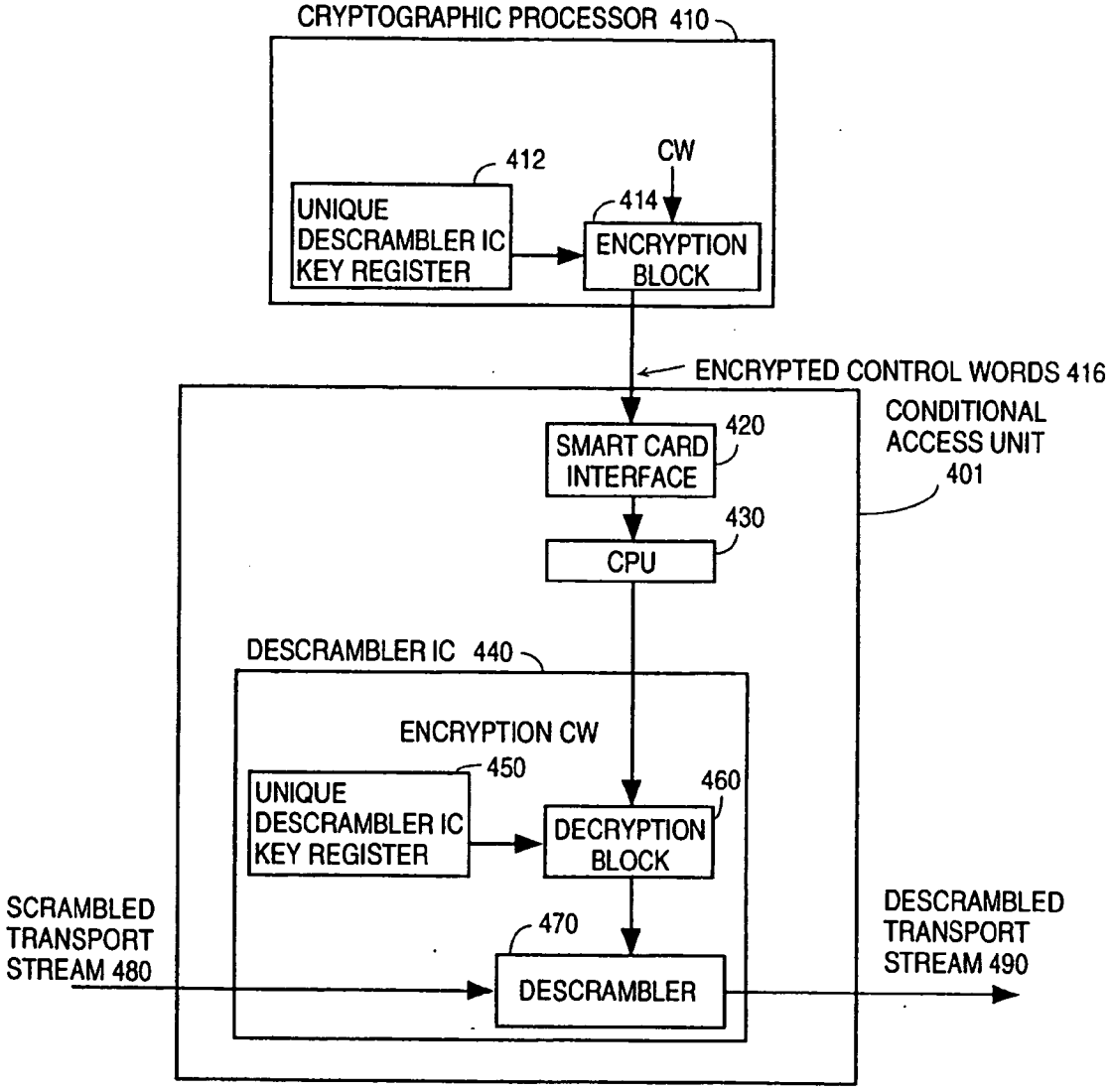

CRYPTOGRAPHIC PROCESSOR 410
412
UNIQUE DESCRAMBLER IC KEY REGISTER
CW
414
ENCRYPTION BLOCK
ENCRYPTED CONTROL WORDS 416
CONDITIONAL ACCESS UNIT
401
SMART CARD INTERFACE
420
430
CPU
DESCRAMBLER IC 440
ENCRYPTION CW
450
UNIQUE DESCRAMBLER IC KEY REGISTER
460
DECRYPTION BLOCK
470
DESCRAMBLER
SCRAMBLED TRANSPORT STREAM 480
DESCRAMBLED TRANSPORT STREAM 490

FIG. 2

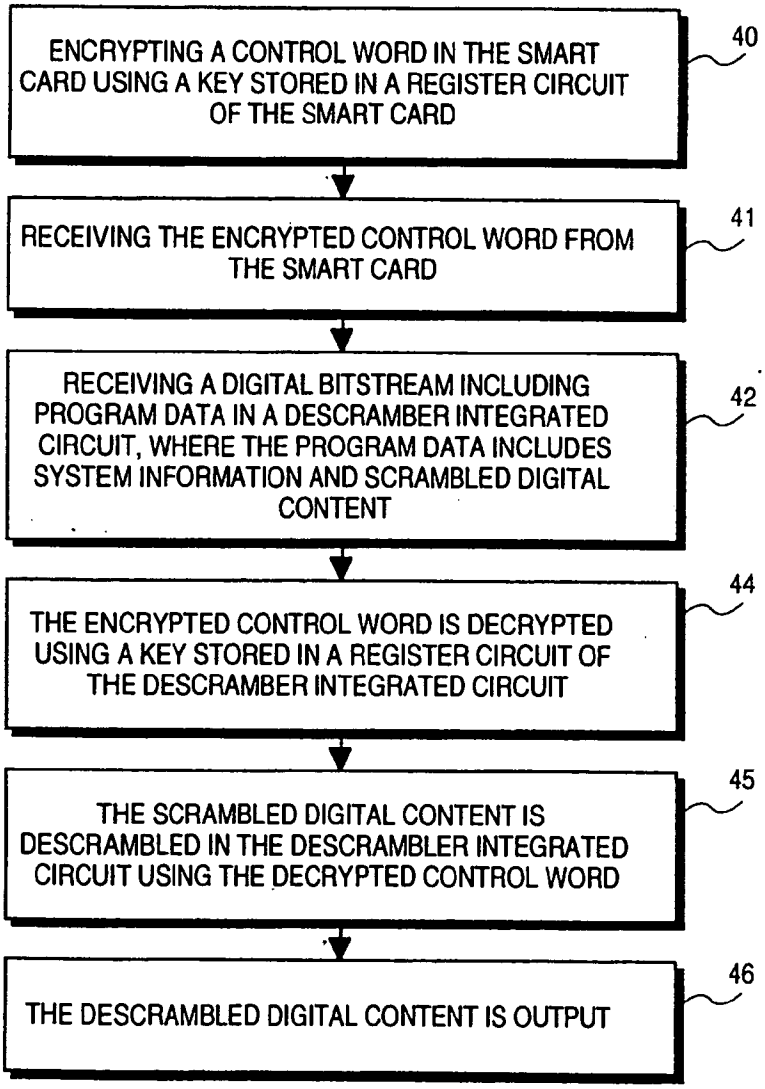

ENCRYPTING A CONTROL WORD IN THE SMART CARD USING A KEY STORED IN A REGISTER CIRCUIT OF THE SMART CARD
40
RECEIVING THE ENCRYPTED CONTROL WORD FROM THE SMART CARD
41
RECEIVING A DIGITAL BITSTREAM INCLUDING PROGRAM DATA IN A DESCRAMBER INTEGRATED CIRCUIT, WHERE THE PROGRAM DATA INCLUDES SYSTEM INFORMATION AND SCRAMBLED DIGITAL CONTENT
42
THE ENCRYPTED CONTROL WORD IS DECRYPTED USING A KEY STORED IN A REGISTER CIRCUIT OF THE DESCRAMBER INTEGRATED CIRCUIT
44
THE SCRAMBLED DIGITAL CONTENT IS DESCRAMBLED IN THE DESCRAMBLER INTEGRATED CIRCUIT USING THE DECRYPTED CONTROL WORD
45
THE DESCRAMBLED DIGITAL CONTENT IS OUTPUT
46

FIG. 3

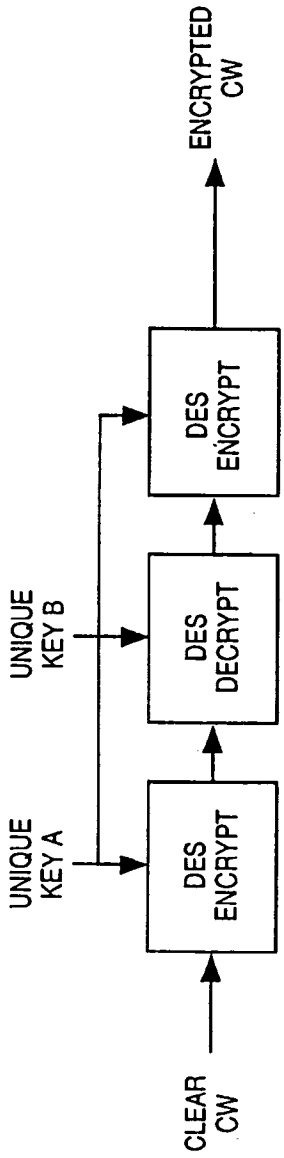

CLEAR CW
UNIQUE KEY A
UNIQUE KEY B
DES ENCRYPT
DES DECRYPT
DES ENCRYPT
ENCRYPTED CW

FIG. 4

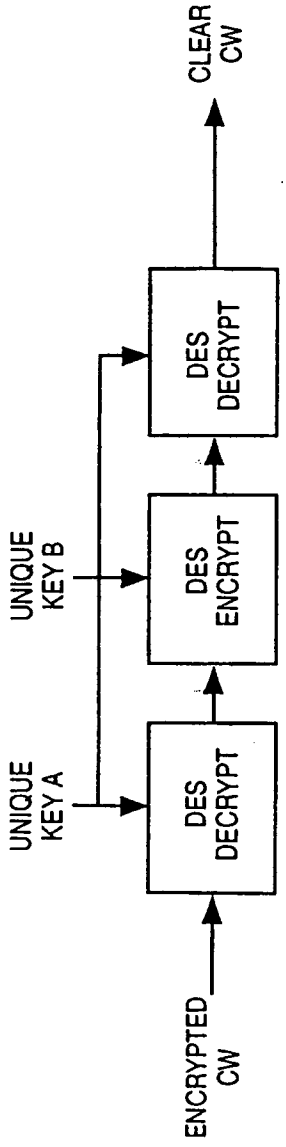

ENCRYPTED CW
UNIQUE KEY A
UNIQUE KEY B
DES DECRYPT
DES ENCRYPT
DES DECRYPT
CLEAR CW

FIG. 5

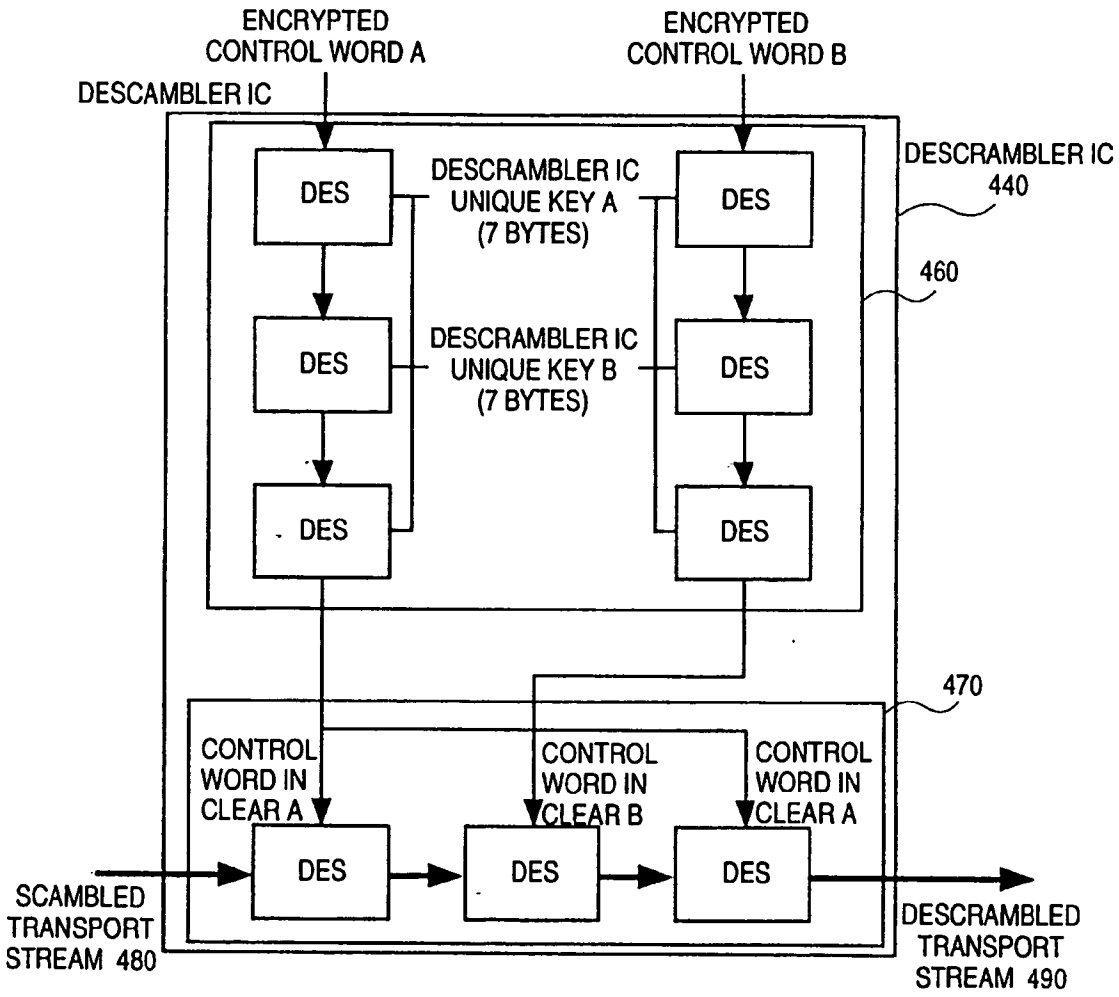

ENCRYPTED CONTROL WORD A
ENCRYPTED CONTROL WORD B
DESCAMBLER IC
DESCRAMBLER IC 440
460
DES
DES
DES
DES
DES
DES
DESCRAMBLER IC UNIQUE KEY A (7 BYTES)
DESCRAMBLER IC UNIQUE KEY B (7 BYTES)
470
CONTROL WORD IN CLEAR A
CONTROL WORD IN CLEAR B
CONTROL WORD IN CLEAR A
DES
DES
DES
SCAMBLED TRANSPORT STREAM 480
DESCRAMBLED TRANSPORT STREAM 490

FIG. 6

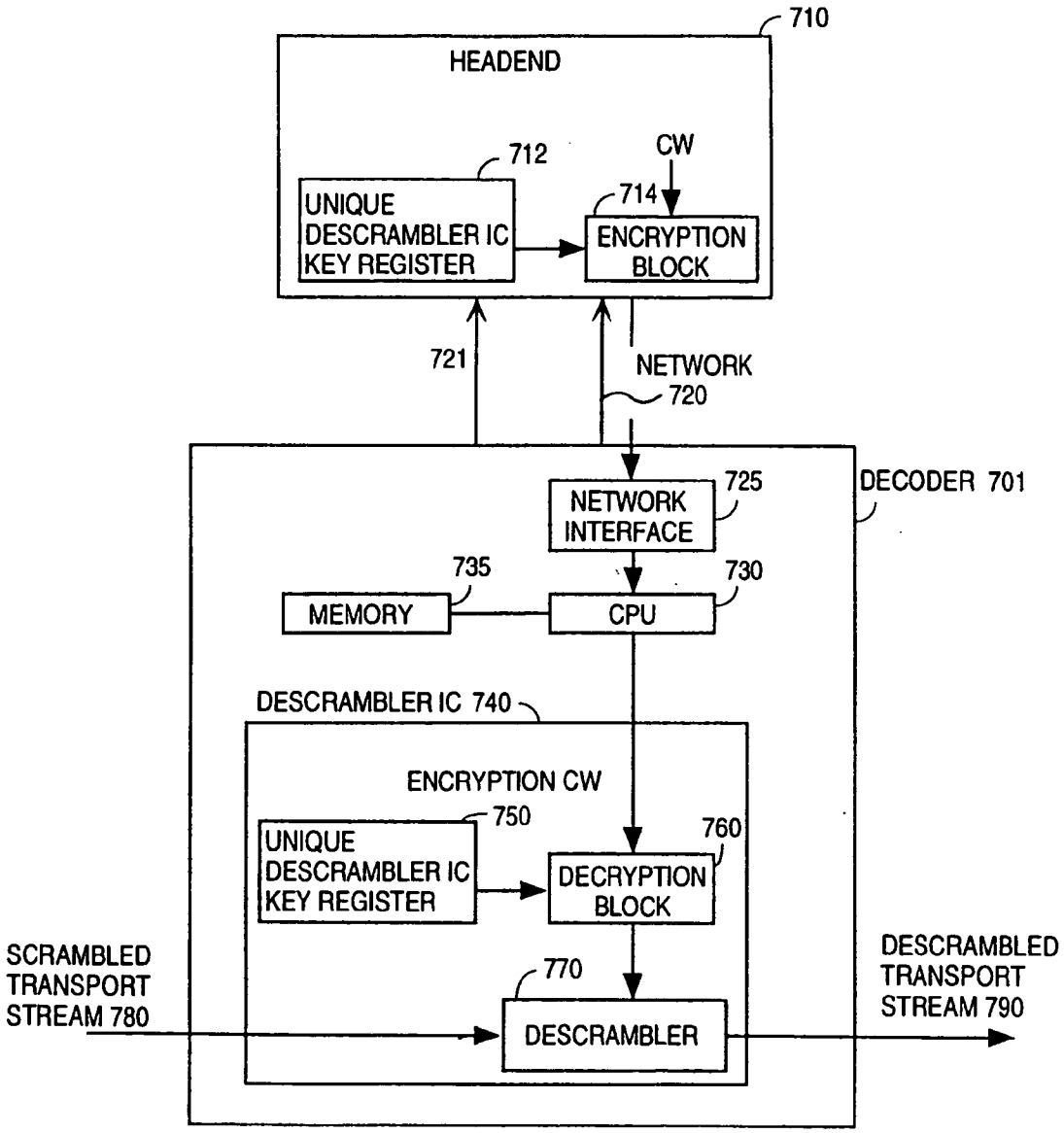

710
HEADEND
712
CW
UNIQUE DESCRAMBLER IC KEY REGISTER
714
ENCRYPTION BLOCK
721
NETWORK
720
DECODER 701
NETWORK INTERFACE
725
735
730
MEMORY
CPU
DESCRAMBLER IC 740
ENCRYPTION CW
750
760
UNIQUE DESCRAMBLER IC KEY REGISTER
DECRYPTION BLOCK
770
SCRAMBLED TRANSPORT STREAM 780
DESCRAMBLER
DESCRAMBLED TRANSPORT STREAM 790

FIG. 7

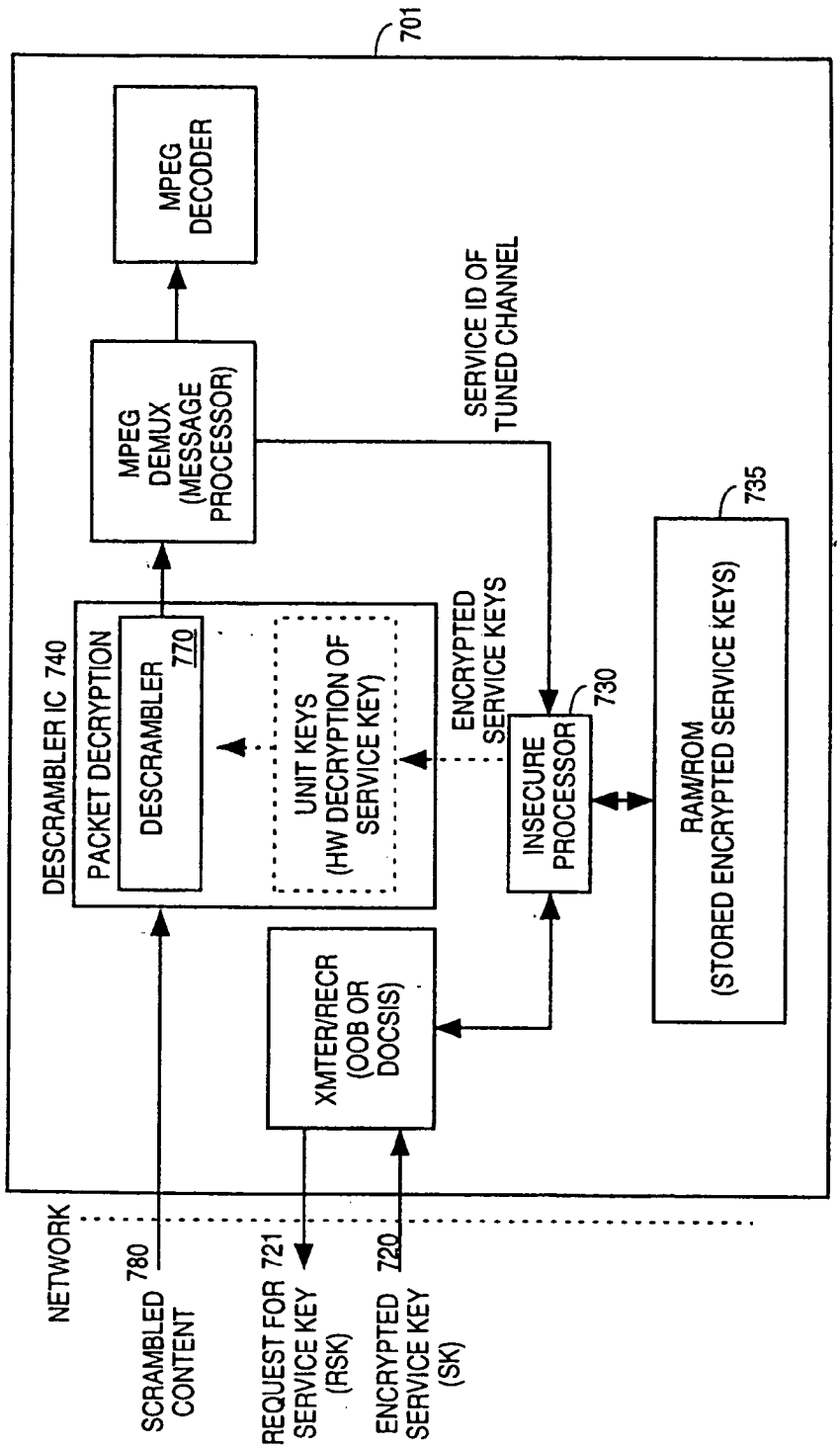

701
MPEG DECODER
MPEG DEMUX (MESSAGE PROCESSOR)
SERVICE ID OF TUNED CHANNEL
DESCRAMBLER IC 740
PACKET DECRYPTION
DESCRAMBLER 770
UNIT KEYS (HW DECRYPTION OF SERVICE KEY)
ENCRYPTED SERVICE KEYS
INSECURE PROCESSOR 730
735
RAM/ROM (STORED ENCRYPTED SERVICE KEYS)
XMTER/RECR (OOB OR DOCSIS)
NETWORK
780
SCRAMBLED CONTENT
REQUEST FOR SERVICE KEY (RSK) 721
ENCRYPTED SERVICE KEY (SK) 720

FIG. 8

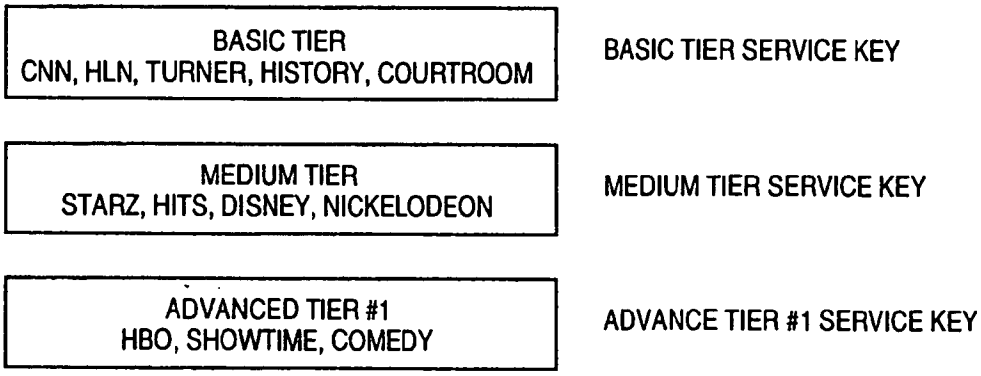

BASIC TIER
CNN, HLN, TURNER, HISTORY, COURTROOM
BASIC TIER SERVICE KEY
MEDIUM TIER
STARZ, HITS, DISNEY, NICKELODEON
MEDIUM TIER SERVICE KEY
ADVANCED TIER #1
HBO, SHOWTIME, COMEDY
ADVANCE TIER #1 SERVICE KEY

FIG. 9

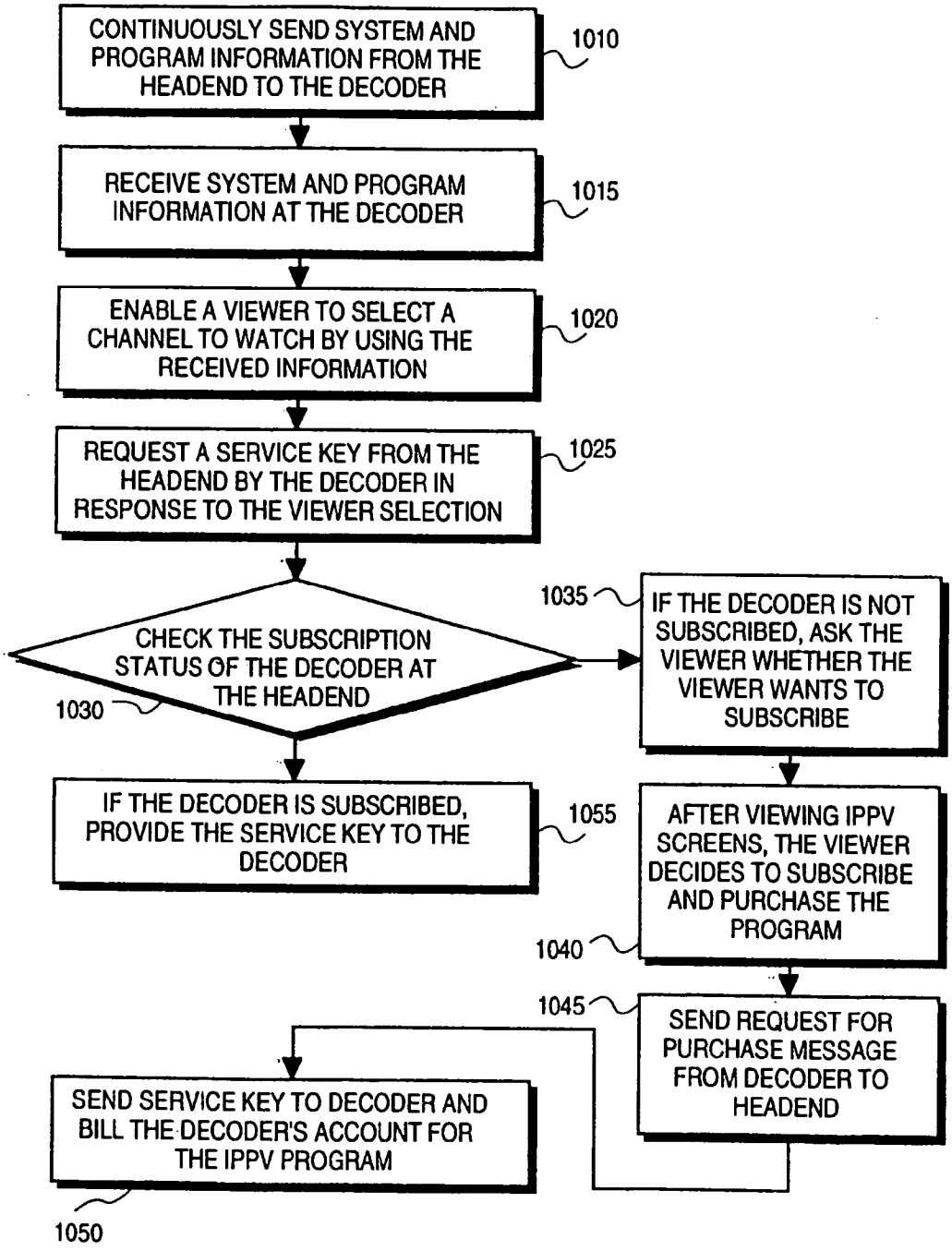

CONTINUOUSLY SEND SYSTEM AND PROGRAM INFORMATION FROM THE HEADEND TO THE DECODER
1010
RECEIVE SYSTEM AND PROGRAM INFORMATION AT THE DECODER
1015
ENABLE A VIEWER TO SELECT A CHANNEL TO WATCH BY USING THE RECEIVED INFORMATION
1020
REQUEST A SERVICE KEY FROM THE HEADEND BY THE DECODER IN RESPONSE TO THE VIEWER SELECTION
1025
CHECK THE SUBSCRIPTION STATUS OF THE DECODER AT THE HEADEND
1030
1035
IF THE DECODER IS NOT SUBSCRIBED, ASK THE VIEWER WHETHER THE VIEWER WANTS TO SUBSCRIBE
IF THE DECODER IS SUBSCRIBED, PROVIDE THE SERVICE KEY TO THE DECODER
1055
AFTER VIEWING IPPV SCREENS, THE VIEWER DECIDES TO SUBSCRIBE AND PURCHASE THE PROGRAM
1040
1045
SEND REQUEST FOR PURCHASE MESSAGE FROM DECODER TO HEADEND
SEND SERVICE KEY TO DECODER AND BILL THE DECODER'S ACCOUNT FOR THE IPPV PROGRAM
1050

FIG. 10

INTERNATIONAL SEARCH REPORT

In tional Application No
PCT/US 00/05111

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, PAJ, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y X	WO 86 07224 A (SCIENTIFIC ATLANTA) 4 December 1986 (1986-12-04) page 8, line 4 - line 29 figures 4,5 --- WO 97 38530 A (DAVIES DONALD WATTS ;GLASSPOOL ANDREW (GB); DIGCO B V (NL); RIX SI) 16 October 1997 (1997-10-16) abstract page 4, line 6 - line 35 figure 1 --- -/--	1-4, 12-15, 23-26 7-9, 18-20, 29,30,33 1,2,5,6, 10-13, 16,17, 21-24, 27,28, 31,32

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 June 2000	04/07/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Masche, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/US 00/05111

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 485 577 A (EYER MARK K ET AL) 16 January 1996 (1996-01-16)	7-9, 18-20, 29,30,33
A	column 4, line 31 - line 46 column 4, line 64 - line 67 column 5, line 11 - line 55 figures 1-3	1-4, 12-15, 23-26
A	EP 0 471 373 A (GEN INSTRUMENT CORP) 19 February 1992 (1992-02-19) abstract column 5, line 41 - line 48 column 6, line 20 - line 28 column 7, line 8 - line 10 column 9, line 16 - line 20 figure 1	1-33
A	EP 0 866 615 A (SONY CORP) 23 September 1998 (1998-09-23) column 8, line 15 - line 22 column 8, line 44 -column 9, line 40 figure 1	1,2,5, 12,13, 16,23, 24,27

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int tional Application No
PCT/US 00/05111

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 8607224 A	04-12-1986	AU 5812086 A	24-12-1986
		EP 0222818 A	27-05-1987
		JP 62503066 T	03-12-1987
		ZA 8602839 A	30-12-1986
WO 9738530 A	16-10-1997	AT 193963 T	15-06-2000
		AU 2506397 A	29-10-1997
		BR 9708500 A	03-08-1999
		CA 2250833 A	16-10-1997
		CN 1215528 A	28-04-1999
		EP 0891670 A	20-01-1999
		HR 970160 A	28-02-1998
US 5485577 A	16-01-1996	AU 693957 B	09-07-1998
		AU 4038995 A	27-06-1996
		CA 2164173 A	17-06-1996
		DE 69515822 D	27-04-2000
		EP 0717566 A	19-06-1996
		JP 8298657 A	12-11-1996
		NO 955100 A	17-06-1996
EP 0471373 A	19-02-1992	US 5111504 A	05-05-1992
		AT 185461 T	15-10-1999
		AU 632704 B	07-01-1993
		AU 8241291 A	20-02-1992
		CA 2049083 A	18-02-1992
		DE 69131680 D	11-11-1999
		DE 69131680 T	11-05-2000
		ES 2137923 T	01-01-2000
		JP 2930149 B	03-08-1999
		JP 4288743 A	13-10-1992
		KR 188425 B	01-06-1999
		NO 179160 B	06-05-1996
EP 0866615 A	23-09-1998	JP 10262013 A	29-09-1998
		CN 1198637 A	11-11-1998